How to setup Web filters in DFL-210/800/1600/2500 VPN Firewall

You can set your firewall to block access to certain Web sites. This setup example shows two ways of setting the filters up:

- A. Blocking specific sites and allowing access to all other Web sites.
- B. Allowing access to specific sites and blocking all other HTTP access;

Step 1. Log into the Firewall by opening Internet Explorer and typing the LAN address of the Firewall. In our example we are using 192.168.1.1. Enter Username and Password which you specified during the initial setup of the Firewall.

Step 2. Click on Objects > Application Layer Gateways. Click on "http-outbound".

D-Link Building Networks for People			9	Logged in as administrator dlink - 59.154.113.18
💁 Home 🛛 🕞 Configuration 🗸 🛛 穬 Tools	s 🗸 🛛 🏐 Status 🗸			🖉 Logout 🛛 🕜 Help
DFL-210 DFL-210 DFL-210 Dects Dojects Address Book Dojects Services Services Schedule Profiles Schedule Profiles DFL-210 Services Dojects Dojects DFL-210 Services Dojects DFL-210 Services Dojects DFL-210 Services DFL-2	Application Layer Application Layer Application Layer Application Layer Add Md Mtp-outbound Add ftp-inbound Application Layer Add H1200 Add H1200 H120	AT ALG_FTP ALG_FTP ALG_FTP ALG_FTP ALG_FTP ALG_H323	ays s) are protocol helpers that can parse complex pr Parameters Strip ActiveX, Strip Java Applets, Strip Sc Client in active mode allowed Server in passive mode allowed Client in active mode allowed, Server in Right-	rotocols, such as HTTP and H.323. Comments ripts passive m click on a row for further options.

Click on "Add" and select "HTTP URL"

	Use an HTTP Application I	ayer Gateway to filter HTTP.	traffic.
Ser.			Edit the settings for this folder
			_
Add 🗕			
Add 🗕	URL		-

Step 3. Setting Blacklists and Whitelists.

There are two ways of setting Web filters:

- A. Blocking specific sites and allowing access to all other Web sites ("Blacklisting"). or
- B. Allowing access to specific sites and blocking all other HTTP access ("Whitelisting");

A. Blocking specific sites and allowing access to all other Web sites (Blacklisting).

When adding the HTTP URL object select "Blacklist" under Action. Enter in the Web site that you want to block. You can use wildcards (*), e.g. *xxx.com/*.

Click on OK.

In an in the second	
Blacklist	URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them. No content filtering
performed on wh	itelist entries, i.e. no active content stripping, blacklist lookups, etc.
Example for allo	wing/preventing all access to a whole site
example.com/*	
.example.com/	
Note the trailing Action:	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positive:
Note the trailing Action: URL:	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positive: Blacklist *xxxx.com/*
Note the trailing Action: URL: Comments	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positive: Blacklist *xxxx.com/*

To add more Web sites click on Add and select HTTP URL and repeat the above step.

Note: You do not need to create an additional Whitelist because by default the firewall allows access to all websites.

B. Allowing access to specific sites and blocking all other HTTP access (Whitelisting).

When adding the HTTP URL object select "Whitelist" under Action. Enter in the Web site that you want to allow access to. You can use wildcards (*), e.g. *google.com.au/*.

Click on OK.

Blacklist content fi	URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them. I iltering is performed on whitelist entries, i.e. no active content stripping, blacklist lookups, etc.
Example for allow	wing/preventing all access to a whole site
example.com/*	
.example.com/	
Note the trailing	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com"
Note the trailing : without false posi Action:	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" itives. Whitelist
Note the trailing : without false posi Action: URL:	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" itives. Whitelist *google.com.au/*
Note the trailing : without false posi Action: URL: Comments	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" itives. Whitelist *google.com.au/*
Note the trailing : without false posi Action: URL: Comments Comments:	slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" itives. Whitelist *google.com.au/*

To add more Web sites click on Add and select HTTP URL and repeat the above step.

When using Whitelisting you need to add an additional HTTP URL entry which will block every other site. Add another HTTP URL and select Blacklist under Action. Under URL enter *.*.*/*.

Click on OK.

General		
Blacklist content f	URLs to deny access to complete filtering is performed on whitelist	e sites, to file types by extension, or to URLs with certain words in them entries, i.e. no active content stripping, blacklist lookups, etc.
Example for allo	wing/preventing all access to a v	hole site
example.com/*		
.example.com/	•	
Note the trailing	slash and double variations to a	low/prevent access to "example.com" as well as "www.example.com"
Note the trailing without false pos Action:	slash and double variations to al sitives. Blacklist	low/prevent access to "example.com" as well as "www.example.com"
Note the trailing without false pos Action: URL:	slash and double variations to a sitives. Blacklist *,*,*/*	low/prevent access to "example.com" as well as "www.example.com"
Note the trailing without false pos Action: URL: Comments	slash and double variations to al sitives. Blacklist *.*.*/*	low/prevent access to "example.com" as well as "www.example.com"
Note the trailing without false pos Action: URL: Comments Comments:	slash and double variations to al sitives. Blacklist *.*.*/*	low/prevent access to "example.com" as well as "www.example.com"

This Blacklist entry should be the last one on the list (the final Blacklist *.*.*/* entry is only required in Example B (Allowing access to specific sites and blocking all other HTTP access). Example A will only have a list of Blacklist entries for specific Web sites.

	Use an HTTP Applicatio	n Layer Gateway to filter HTTP traffic.	
100			Edit the settings for this folder
Add	*		
bbA C	▼	(21353)-1-4	
bbA (▼ Action ▼	URL 🕶	Comments 🔻
bbA (Action -	URL ▼ *google.com.au/*	Comments 🔻

Step 4. Add an IP Rule. Go into Rules > IP Rules. Click on "Add" and select "IP Rule".



Specify the following settings for the new IP Rule: Name: (in our example we used "ALG") Action: NAT Service: http-outbound (the Application Layer Gateway we configured in the previous steps) Source Interface: Ian; Source Network: Iannet Destination Interface: any; Destination Network: all-nets



Step 5. Move the rule to the top of the list.

Right click on the new IP Rule "ALG" and select "Move to Top".

8 IP Rules are used to filter IP-bas	ed network traffic. In addition.	they provide means for	address translation as well as	Server Load Balancin
•				
J Add ▼				
▼ Name ▼ Action ▼ Source	ceInterface 💌 SourceNetwo	ork 🔻 DestinationIr	terface 🔻 DestinationNet	work 🔻 Service 💌
🖁 ping_fw Allow lan	lannet	core	lan_ip	ping- inbound
😫 lan_to_wan1				
A Fdit	lannet	any	all-nets	http- outbound
2 Delete	-		() Right-click on a	row for further options
Delete	-			
Move to Top				

1	IP Rules are	e used to filt	er IP-based netwo <mark>rk</mark> ti	raffic. In addition, they p	provide means for address tra	inslation as well as Server I	Load Balancin
) A	dd -						
• •	Name 🔻	n	 SourceInterface 	SourceNetwork 🔻	DestinationInterface 💌	DestinationNetwork 💌	Service 🔻
)	8 ALG	NAT	lan	lannet	any	all-nets	http- outbound
	g ping_fw	Allow	lan	lannet	core	lan_ip	ping- inbound

Step 6. Save the new configuration. In the top menu bar click on Configuration and select "Save and Activate".



Click on OK to confirm the new settings activation:

D-Link Building Networks for People		Cogged in as administrator edmin - 192.168.1.2
🔮 Home 🛛 📑 Configuration 👻 🎢 To	ils 👻 🥶 Status 👻	😕 Logout 🕜 Help
DFL-210 DFL-210 DFL-210 DFL-20 DFL	Save Configuration Provide the state of the state	uration. Otherwise the unit will assume that you accidentally looked

Wait 15 seconds for the Firewall to apply the new settings.